Binary singly even self-dual code に関連した extremal problem(組合せデザインとその周辺における数理的基礎およびそれらの応用)

AUTHOR(S):

宗政, 昭弘

CITATION:

宗政, 昭弘. Binary singly even self-dual code に関連した extremal problem(組合せデザインとその周辺における数理的基礎およびそれらの応用). 数理解析研究所講究録 2006, 1465: 130-137

ISSUE DATE:

2006-01

URL:

http://hdl.handle.net/2433/48023

数理解析研究所講究録 1465 巻 2006 年 130-137

Binary singly even self-dual code に関連した extremal problem

東北大学大学院情報科学研究科　宗政昭弘（Akihiro MUNEMASA）
Graduate School of Information Sciences,
Tohoku University

2005年8月4日

1 A packing problem

通常、組合せデザイン理論においては、packing problem とは次のような問題である。Ω_v を v-element set とし、k, λ を正の整数とする。このとき、Ω_v の k-element subset の family $\mathcal{B} \subset \binom{\Omega_v}{k}$ で、$\mathcal{B}$ の異なる2つの member は高々 λ 点で交わるようなもののサイズ $|\mathcal{B}|$ の最大値を求めよ。

この問題を解くことによって、binary code の weight distribution に制限を与えることができる。C を最小 weight が d の binary linear code とし、$\boldsymbol{u}, \boldsymbol{v}$ を C の weight w の異なる codeword とする。このとき、

$$|\mathrm{supp}(\boldsymbol{u}) \cap \mathrm{supp}(\boldsymbol{v})| \leq w - \frac{d}{2}$$

が成り立つ。実際そうでないとすると $\boldsymbol{u}+\boldsymbol{v}$ の weight が d より小さくなってしまうからである。Codeword とその support を同一視することにすれば、前述の問題の解から C の weight w の codeword の個数の上界が得られることになる。

このような上界を得るための常套手段は linear programming bound である（Delsarte [1]）。$\mathcal{B} \subset \binom{\Omega_v}{k}$ で、$L \subset \{0, 1, \ldots, k-1\}$ に対して

$$B, B' \in \mathcal{B},\ B \neq B' \implies |B \cap B'| \in L$$

を満たすとすると、$|\mathcal{B}|$ は

$$\max\{\sum_{i=0}^{k} a_i \mid (a_0, a_1, \ldots, a_k)Q \geq 0,\ a_0 = 1,\ a_{k-i} = 0\ (i \notin L),\ a_j \geq 0\ (\forall j)\}$$

で上から押さえられる。ただし、Q は $(k+1)\times(k+1)$ 行列でその成分は

$$Q_{ij}=\left(\binom{v}{j}-\binom{v}{j-1}\right)\sum_{r=0}^{j}(-1)^r\frac{\binom{i}{r}\binom{j}{r}\binom{v+1-j}{r}}{\binom{k}{r}\binom{v-k}{r}}\qquad(0\le i,j\le k).\tag{1}$$

例として、$v=62$, $k=7$, $\lambda=1$ の場合を考えよう。後でこの値を binary self-dual $[62,31,12]$ code に応用したいのでこのような v,k,λ を考えるのである。この場合、$L=\{0,1\}$ なので

$$|\mathcal{B}|\le\max\{1+a+b\mid(1,0,0,0,0,0,a,b)Q\ge 0,\ a\ge 0,\ b\ge 0\}$$

となる。Q を計算して条件を書けば

$$\begin{aligned}13a-49b&\ge-385,\\-73a+49b&\ge-3465\end{aligned}$$

となる。図を書いて考えれば $1+a+b$ の最大値は、(a,b) が2直線 $13a-49b=-385$, $-73a+49b=-3465$ の交点 $(\frac{385}{6},\frac{1045}{42})$ においてとることがわかる。これより、

$$|\mathcal{B}|\le 1891/21\tag{2}$$

となり、$|\mathcal{B}|\le 90$ がわかる。

この講演の終了後、徳重典英氏より、同じ上界は簡単な数え上げからも得られるというコメントがあったので、ここに記しておく。一般に、高々 λ 点で交わるような family $\mathcal{B}$ については、

$$|\{(A,B)\mid A\in\binom{\Omega_v}{\lambda+1},\ B\in\mathcal{B},\ A\subset B\}|$$

を2通りに数えることによって不等式

$$|\mathcal{B}|\binom{k}{\lambda+1}\le\binom{v}{\lambda+1}$$

が得られる。$(v,k,\lambda)=(62,7,1)$ とすれば (2) が得られるのである。

2 Binary self-dual codes

さて、この問題を binary self-dual code へ応用するために、必要な定義をする。

Binary $[n,k]$ code C とは $\mathbb{F}_2^n$ の k 次元部分ベクトル空間のことである。ただしここで $\mathbb{F}_2$ は2元体である。本稿では、すべての code は binary とする。n は code の長

さと呼ばれる。$\mathbb{F}_2^n$ のベクトル $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$ に対し、座標 j で $u_j = 1$ となるようなものの集合を u の support という。u の weight とは support のサイズのことである。Code C の元は codeword と呼ぶ。C の minimum weight とは C の nonzero codeword の weight の最小値である。Minimum weight が d の $[n, k]$ code を $[n, k, d]$ code とも書く。y を不定元とするとき、code C の weight enumerator W_C とは、y の多項式 $W = \sum A_i y^i$ であり、ここで A_i は weight i の codeword の数である。

Code C の dual code $C^\perp$ とは

$$C^\perp = \{\boldsymbol{u} \in \mathbb{F}_2^n | \ (\boldsymbol{u}, \boldsymbol{v}) = 0 \text{ for all } \boldsymbol{v} \in C\}$$

で定義されるものである。ここで $(\boldsymbol{u}, \boldsymbol{v})$ は通常の内積である。C は $C = C^\perp$ を満たすとき self-dual と呼ばれる。Self-dual code C が doubly even とは、すべての codewords の weight が $\equiv 0 \pmod 4$ を満たすときであり、そうではないときは singly even と呼ばれる。

特に singly even self-dual code を研究するのに欠かせないのが Conway and Sloane [2] によって導入された shadow の概念である。C を singly even self-dual code とし、C_0 を weight $\equiv 0 \pmod 4$ となる codewords からなる subcode とする。このとき、C_0 は C において codimension 1 の subcode になる。C の shadow S とは $C_0^\perp \setminus C$ をさす。明らかに $|C| = |S|$ である。また、C_0 の cosets C_1, C_2, C_3 が存在して $C_0^\perp = C_0 \cup C_1 \cup C_2 \cup C_3$ ただし $C = C_0 \cup C_2$ and $S = C_1 \cup C_3$ となる。この番号の付け方、つまり C に含まれる coset を C_2 とするのは、$n \equiv 2 \pmod 4$ の場合に、S には奇数 weight のベクトルが含まれることを連想しやすくするためである。実際、S に含まれるベクトルの weight は mod 4 で $\frac{n}{2}$ に合同であることが知られている。このことはもっと強い、weight enumerator の次の公式からわかる。C を self-dual code とすると、C の weight enumerator W_C は

$$W_C = \sum_{j=0}^{[n/8]} a_j (1 + y^2)^{n/2-4j} (y^2(1 - y^2)^2)^j$$

という形に書ける。このとき S の weight enumerator は

$$W_S = \sum_{j=0}^{[n/8]} a_j (-1)^j 2^{n/2-6j} y^{n/2-4j} (1 - y^4)^{2j}$$

となり、W_S に現れる項の y の次数は mod 4 で $n/2$ に合同であることがわかる。

長さ n の self-dual code C の minimum weight d は

$$d \leq \begin{cases} 4[n/24] + 4 & n \not\equiv 22 \pmod{24}, \\ 4[n/24] + 6 & n \equiv 22 \pmod{24}. \end{cases}$$

をみたし ([4, 5])、上の不等式で等号が成立するとき、extremal という。Extremal self-dual code を同値を除いてすべて決定するというのは、自然な流れであるが、この問題は長さ n によって難易度がいろいろ変わるだけでなく、存在する extremal code の個数も大きく変わる。

S は C の coset であるから、距離空間としては C と同型なわけで、これは S の異なる2つのベクトルの Hamming 距離も C と同じく、d 以上であることを意味する。したがって

$$B_r \leq A(n, d, r)$$

となる。ここで、$A(n, d, w)$ は長さ n, weight w で Hamming distance が少なくとも d 離れているような binary vector の集合のサイズの最大値である。しかし $A(n, d, r)$ は n, d, r が小さい時、または特別な場合を除いて、決定するのは難しい。

3 Self-dual $[62, 31, 12]$ codes

例として self-dual $[62, 31, 12]$ code を考える。この場合、shadow のベクトルの weight は 3 (mod 4) であるが、shadow の minimum weight が 3 でない場合、weight enumerator は次のようになる。

$$W_C = 1 + (1860 + 32\beta)y^{12} + (28055 - 160\beta)y^{14} + \cdots, \tag{3}$$
$$W_S = \beta y^7 + 12(93 - \beta)y^{11} + \cdots$$

W_S の係数は非負整数でなければならないので、$0 \leq \beta \leq 93$ である。S の異なる2つのベクトルの Hamming 距離も C と同じく、12 以上であるので、linear programing bound で示した通り $\beta \leq 90$ である。

この講演の目的は、この β の上界を改良する方法を紹介することである。Shadow は2つの coset C_1, C_3 からなっているが、上述の上界は、この事実を全く使っていない。C_1, C_3 それぞれも minimum distance が 12 であるから、C_1 (または C_3) に属する weight 7 の異なる2つのベクトルは support が高々1点でしか交わらない。しかしもし support の交わりが空だとするとそれらの和は weight 14 になるが、C_1 の2つのベクトルの和は C_0 に入らなければならないので、weight は 4 の倍数であり、これは矛盾である。したがって、C_1 に属する weight 7 のベクトルは、どの2つもその support がちょうど1点で交わる、という性質を持つことがわかる。これは $L = \{0, 1\}$ ではなく、$L = \{1\}$ として linear programming bound を適用すべきであったということを意味している。

一方、C_1 のベクトルと C_3 のベクトルの和は C_2 に属し、従ってその weight は $\equiv 2$ (mod 4) である。C_2 の minimum weight は 14 であるから、C_1 に属する weight 7 の

ベクトルと C_3 に属する weight 7 のベクトルは disjoint な support を持つことになる。そこで、

$$\begin{aligned}
\mathcal{B}^{(1)} &= \{\mathrm{supp}(\boldsymbol{u}) \mid \boldsymbol{u} \in C_1,\ \mathrm{wt}(\boldsymbol{u}) = 7\},\\
\mathcal{B}^{(3)} &= \{\mathrm{supp}(\boldsymbol{u}) \mid \boldsymbol{u} \in C_3,\ \mathrm{wt}(\boldsymbol{u}) = 7\},\\
\mathcal{B} &= \mathcal{B}^{(1)} \cup \mathcal{B}^{(3)} \subset \binom{\Omega_{62}}{7},\\
\Omega^{(1)} &= \bigcup_{B \in \mathcal{B}^{(1)}} B,\\
\Omega^{(3)} &= \bigcup_{B' \in \mathcal{B}^{(3)}} B'
\end{aligned}$$

とおくと、

$$\Omega^{(1)} \cap \Omega^{(3)} = \emptyset, \qquad \Omega^{(1)} \cup \Omega^{(3)} \subset \Omega_{62}$$

となる。さて、$\beta = |\mathcal{B}| = |\mathcal{B}^{(1)}| + |\mathcal{B}^{(3)}|$ の上界を得るためには、$|\mathcal{B}^{(1)}|$, $|\mathcal{B}^{(3)}|$ それぞれの上界を求めれば良いが、これらは $v^{(i)} = |\Omega^{(i)}|$ に依存する。$|\mathcal{B}^{(i)}|$ の上界は

$$M(v^{(i)}) := \max\{1 + a \mid (1,0,0,0,0,0,a,0)Q_{v^{(i)}} \geq 0,\ a \geq 0\}$$

で与えられる。ただし $Q_{v^{(i)}}$ は (1) において $v = v^{(i)}$, $k = 7$ とおいた式で与えられる行列である。すると

$$\begin{aligned}
\beta &\leq M(v^{(1)}) + M(v^{(3)})\\
&\leq \max\{M(v) + M(62 - v) \mid 0 \leq v \leq 62\}\\
&= 48.
\end{aligned}$$

となる。ただし、$M(v)$ は $v \leq 13$ の時は、

$$M(v) := \begin{cases} 2 & \text{if } v = 13,\\ 1 & \text{if } 7 \leq v \leq 12,\\ 0 & \text{if } 0 \leq v \leq 6 \end{cases}$$

と定義しておく。

以上により、$\beta \leq 48$ が得られた。また、$\beta = 48$ となり得るのは $\{v^{(1)}, v^{(3)}\} = \{0, 62\}$, $\{1, 61\}$ の場合のみであることもわかる。特に $\beta = 48$ なら $\mathcal{B}^{(1)} = \emptyset$ または $\mathcal{B}^{(3)} = \emptyset$ となる。

(3) 式を weight enumerator にもつ self-dual $[62, 31, 12]$ code については、$\beta = 0, 10, 15$ となる例のみが知られている (Dontcheva–Harada [3])。

4 Self-dual $[42, 21, 8]$ codes

もうひとつ、簡単な例として $[42, 21, 8]$ code を考えよう。この場合はとてもきれいに特徴付けができる。

$$W_C = 1 + (84 + 8\beta)y^8 + (1449 - 24\beta)y^{10} + \cdots \tag{4}$$

$$W_S = \beta y^5 + (896 - 8\beta)y^9 + \cdots \tag{5}$$

上と同様の議論により、shadow における weight 5 の vector は、$\mathcal{B}^{(1)}, \mathcal{B}^{(3)}$ の 2 つに分かれ、それぞれにおいてはちょうど 1 点で support が交わり、異なる part に属する vector は disjoint な support を持つ。したがって上と同様にして上界が計算できる。上界は 42 となり、等号成立は $|\mathcal{B}^{(1)}| = |\mathcal{B}^{(3)}| = 21$ の時に限り、このときは $\mathcal{B}^{(1)} \cong \mathcal{B}^{(3)} \cong PG(2, 4)$ となる。すると、C_0 はこれらと直交していなければならないが、これらと直交する weight 8 のベクトルはちょうど 420 個あることが計算機により確かめられる。C_0 は (4) により weight 8 の codeword を 420 個含まなければならないのでこれらをすべて含む。これら 420 個のベクトルは 18 次元の部分空間を生成する。$\dim C_0 = 20$ なので、あと 2 次元拡大しなければならない。この拡大の仕方は一意的ではないが、すべて同値であることが計算機により確かめられる。以上より (4) で $\beta = 42$ となる code は一意的であることが示された。

5 Magma program

まず、行列 Q の成分を定義しておく。

```
HahnPolynomial:=function(v,k,l,x)
    return (Binomial(v,l)-Binomial(v,l-1))*
        &+[ (-1)^i*Binomial(l,i)*Binomial(v+1-l,i)*
            Binomial(k,i)^(-1)*Binomial(v-k,i)^(-1)*
            Binomial(x,i) : i in [0..l] ];
end function;
Qmatrix:=function(v,k)
   return Matrix(Rationals(),k+1,k+1,
       [ [ HahnPolynomial(v,k,l,x) : l in [0..k] ]
          : x in [0..k] ] );
end function;
```

次に $k = 7$ の場合の上界を定義し、これを計算する。

```
boundM:=function(v)
    if v le 6 then
        return 0;
    elif v le 12 then
        return 1;
    elif v eq 13 then
        return 2;
    else
        Q:=Qmatrix(v,7);
        return Min( { 1-Q[1][i+1]/Q[7][i+1]
            : i in [0..7] | Q[7][i+1] lt 0 } );
    end if;
end function;
bounds:=[ Floor(boundM(v)+boundM(62-v))
    : v in {0..31} ];
max:=Max(bounds);
max eq 48;
[ v : v in [0..31] | max eq bounds[v+1] ] eq [0,1];
```

次に、$[42, 21, 8]$ code with $\beta = 42$ の特徴付けのためのプログラムを述べる。

まず、2つの disjoint な $PG(2,4)$ で生成される code を定義し、これを S とおく (S は shadow ではない)。求める code C はこの code の dual に含まれているからである。

```
M21:=KMatrixSpace(GF(2),21,21);
In21:=M21!IncidenceMatrix(FiniteProjectivePlane(GF(4)));
S:=LinearCode(VerticalJoin(
   HorizontalJoin(M21!0,In21),
   HorizontalJoin(In21,M21!0) )
   );
```

この S の dual にはちょうど 420 個の weight 8 の codeword が含まれている。また、これらで生成される S の dual の subcode S0 は次元が 18 であることがわかる。

```
DualS:=Dual(S);
NumberOfWords(DualS,8) eq 420; // beta=42
S0:=sub< DualS | Words(DualS,8) >;
Dimension(S0) eq 18;
S0p:=Dual(S0);
```

したがって、求める code C はこの 18 次元 code S0 を含み、また S0 の dual である 24 次元 code S0p に含まれる。それらを W_{18}, W_{24} とおく。

```
V42:=VectorSpace(GF(2),42);
W18:=sub< V42 | S0 >;
W24:=sub< V42 | S0p >;
```

W_{24} に含まれ、W_{18} を含む 20 次元 doubly even code で minimum weight が 8 となるものをすべて列挙する（そのような code は W_{18} に W_{24} のベクトル 2 つを付け加えて得られる）。

```
W24byW18de:=[ x : x in Transversal(W24,W18) |
   (x ne 0) and (Weight(x) mod 4 eq 0) ];
j:=V42![1: i in [1..42]];
W20s:=[ LinearCode(sub< W24 | W18,x,y >) :
   x in W24byW18de, y in W24byW18de
   | ((x,y) eq 0) and Dimension(sub< W24 | W18,x,y >) eq 20
   and MinimumWeight(LinearCode(sub< V42 | W18,x,y,j>)) eq 8 ];
```

最後に、これらがすべて同値な code になっていることを確認する。

```
&and{ IsIsomorphic(W20s[1],W20s[i]) : i in [2..#W20s] };
```

参考文献

[1] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Research Reports Suppl. **10** (1973).

[2] J.H. Conway and N.J.A. Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Trans. Inform. Theory* **36** (1990), 1319–1333.

[3] R. Dontcheva and M. Harada, New extremal self-dual codes of length 62 and related extremal self-dual codes, *IEEE Trans. Inform. Theory* **48** (2002), 2060–2064.

[4] C.L. Mallows and N.J.A. Sloane, An upper bound for self-dual codes, *Inform. Control* **22** (1973), 188–200.

[5] E.M. Rains, Shadow bounds for self-dual codes, *IEEE Trans. Inform. Theory* **44** (1998), 134–139.